

7/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:Derwent WPI
(c) 2002 Derwent Info Ltd. All rts. reserv.

013183164 **Image available**
WPI Acc No: 2000-355037/ 200031
XRPX Acc No: N00-266141

**Prepaid electronic cash system indicates praxis of settlement-of-accounts
to settlement-of-accounts processor based on account number of payment
system**

Patent Assignee: SONY CORP (SONY)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 2000113085	A	20000421	JP 98286341	A	19981008	200031 B

Priority Applications (No Type Date): JP 98286341 A 19981008

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2000113085	A		19	G06F-019/00	

Abstract (Basic): JP 2000113085 A

NOVELTY - A settlement-of-accounts unit (55) shows settlement-of-accounts to a payment system. User management unit (35) manages account number of user's payment system. A communication unit (37) shows changes in balance of prepayment of user, based on identification information of the user. The praxis of settlement-of-accounts is indicated to settlement-of-accounts processor based on account of payment system.

DETAILED DESCRIPTION - An account management unit (45) stores information which identifies the user and balance money of the user on the basis of prepayment money. The encryption is performed by user's payment system with disclosure key information which identifies user and a settlement-of-accounts processor.

USE - Prepaid electronic cash system for processing money to be paid.

ADVANTAGE - The praxis of the settlement-of-accounts is indicated to a settlement-of-accounts processor on the basis of account number of payment system. Therefore, the necessity for managing a special apparatus by the user is eliminated. Utilization of cash is performed safely.

DESCRIPTION OF DRAWING(S) - The figure shows the components of prepaid electronic cash system.

User management unit (35)
Communication unit (37)
Account management unit (45)
Settlement-of-accounts unit (55)
pp; 19 DwgNo 1/9

Title Terms: PREPAYMENT; ELECTRONIC; CASH; SYSTEM; INDICATE; SETTLE;
ACCOUNT; SETTLE; ACCOUNT; PROCESSOR; BASED; ACCOUNT; NUMBER; PAY; SYSTEM
Derwent Class: P85; T01; T05

International Patent Class (Main): G06F-019/00

International Patent Class (Additional): G06F-017/60; G07F-019/00;

G09C-001/00

File Segment: EPI; EngPI

7/5/2 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2002 JPO & JAPIO. All rts. reserv.

06527364 **Image available**
ELECTRONIC CASH SYSTEM

PUB. NO.: 2000-113085 A]

PUBLISHED: April 21, 2000 (20000421)
INVENTOR(s): MATSUYAMA SHINAKO
APPLICANT(s): SONY CORP
APPL. NO.: 10-286341 [JP 98286341]
FILED: October 08, 1998 (19981008)
INTL CLASS: G06F-019/00; G06F-017/60; G07F-019/00; G09C-001/00

ABSTRACT

PROBLEM TO BE SOLVED: To make usable electronic cash in safety without requiring any special device, to disable individual information and individual purchase information to be grasped unnecessarily, and to make the detectable an illegal act and controllable over the circulation of money.

SOLUTION: An account management part 45 stores information for identifying users and the amounts of money spent by the users on a prepayment basis. An adjustment part 55 instructs a payment institution to settle the accounts. A user management part 35 manages the information for identifying the users and the account numbers of the users at the payment institution which are ciphered with an open key of a settlement processor and a communication part 37 indicates alterations of the balances of prepayment of the users stored in an account management device according to the information for identifying the users and instructs the settlement processor to settle the accounts.

COPYRIGHT: (C)2000, JPO

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2000-113085
(P2000-113085A)

(43)公開日 平成12年4月21日(2000.4.21)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード(参考)	
G 0 6 F 19/00		G 0 6 F 15/30	3 6 0	3 E 0 4 0
	17/60	G 0 9 C 1/00	6 4 0 A	5 B 0 4 9
G 0 7 F 19/00			6 6 0 C	5 B 0 5 5
G 0 9 C 1/00	6 4 0		6 6 0 G	
	6 6 0	G 0 6 F 15/21	3 4 0 A	
審査請求 未請求 請求項の数 3 O L (全 19 頁) 最終頁に続く				

(21)出願番号 特願平10-286341

(22)出願日 平成10年10月8日(1998.10.8)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 松山 科子

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74)代理人 100082131

弁理士 稲本 義雄

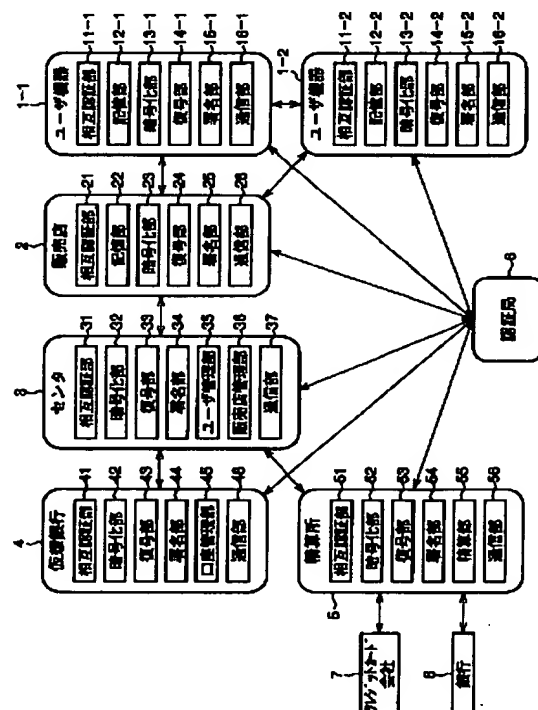
最終頁に続く

(54)【発明の名称】 電子現金システム

(57)【要約】

【課題】 特殊な装置を必要とせず、安全に電子現金の利用ができ、個人の情報および個人の購入情報が不必要に把握できず、不正の検出および金銭の流通が管理できるようにする。

【解決手段】 口座管理部45は、利用者を識別する情報および前払いの代金を基にした利用者の利用金額を記憶する。精算部55は、支払機関に決済を指示する。ユーザ管理部35は、利用者を識別する情報および決済処理装置の公開鍵で暗号化された利用者の支払機関の口座番号を管理し、通信部37は、利用者を識別する情報を基に、口座管理装置が記憶する利用者の前払いの残高の変更を指示し、支払い機関の口座番号を基に、決済処理装置に決済の実行を指示する。



【特許請求の範囲】

【請求項 1】 口座管理装置、決済処理装置、および制御装置からなる、前払いにより代金の支払いを処理する電子現金システムにおいて、

前記口座管理装置は、

利用者を識別する情報、および前記前払いの代金を基にした前記利用者の利用金額を記憶する記憶手段を備え、

前記決済処理装置は、

支払機関に決済を指示する決済指示手段を備え、

前記制御装置は、

利用者を識別する情報、および前記決済処理装置の公開鍵で暗号化された利用者の支払機関の口座番号を管理する管理手段と、

前記管理手段が管理する前記利用者を特定する情報を基に、前記口座管理装置の前記記憶手段が記憶する前記利用者の前記前払いの残高の変更を指示する残高変更指示手段と、

前記管理手段が管理する前記支払い機関の口座番号を基に、前記決済処理装置の前記決済指示手段に決済の実行を指示する決済実行指示手段とを備えることを特徴とする電子現金システム。

【請求項 2】 前記口座管理装置、決済処理装置、および制御装置は、通信の前に所定の相互認証処理を実行することを特徴とする請求項 1 に記載の電子現金システム。

【請求項 3】 前記口座管理装置、決済処理装置、および制御装置の間で送信されるデータは、暗号化されていることを特徴とする請求項 1 に記載の電子現金システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子現金システムに関し、特に、前払いにより代金の支払いを処理する電子現金システムに関する。

【0002】

【従来の技術】電子現金システムの現金の管理方式は、耐タンパー性のある機器を利用し、残高が改竄出来ないことを前提とし、残高を管理する「残高管理方式」と、センターで発行した現金のIDを管理し、二重使用されていないかのチェックを行うために、電子現金に、額面および識別番号を持たせる「電子紙幣方式」に大別される。

【0003】電子現金システムを実用に供するためには、ユーザの個人情報および購入情報に対する匿名性、並びに任意のユーザ機器および販売店などの間で金銭の移動が可能なオープンループ型流通の実現が必要である。

【0004】電子現金システムで、上記の要件を満足しているのは、Mondex（商標）のみである。Mondexでは、サービスを受けるユーザ機器、および商品を提供する販

売店は、それぞれMondexカードを保持し、販売店はさらに、Mondexカードを読み書きするための特殊な装置が必要であり、それを用いて電子現金の入出金を行う。

【0005】インターネット上でのMondexの利用の安全性は、暗号モジュールを常に2つ用意し、安全が保証される方に切り替えて利用するなど、安全性を強化したMondexカードの安全性に依存している。また、Mondexのシステムは、取り引き情報を一切管理しないため、個人の情報および購入履歴は、その匿名性が保たれる。

【0006】

【発明が解決しようとする課題】しかしながら、Mondexのシステムでは、販売店は、特殊な装置を管理する必要があり、手間がかかる。また、取り引き情報を一切管理しないため、不正利用があった際、その検出は出来ず、さらに、金銭の流通が、管理出来ない。

【0007】本発明はこのような状況に鑑みてなされたものであり、特殊な装置を管理する必要がなく、安全に電子現金の利用ができ、個人の情報および個人の購入情報を各装置が不必要に把握できず、不正の検出が可能で、金銭の流通が管理できるようにすることを目的とする。

【0008】

【課題を解決するための手段】請求項 1 に記載の電子現金システムは、口座管理装置が、利用者を識別する情報、および前払いの代金を基にした利用者の利用金額を記憶する記憶手段を備え、決済処理装置が、支払機関に決済を指示する決済指示手段を備え、制御装置が、利用者を識別する情報、および決済処理装置の公開鍵で暗号化された利用者の支払機関の口座番号を管理する管理手段と、管理手段が管理する利用者を特定する情報を基に、口座管理装置の記憶手段が記憶する利用者の前払いの残高の変更を指示する残高変更指示手段と、管理手段が管理する支払い機関の口座番号を基に、決済処理装置の決済指示手段に決済の実行を指示する決済実行指示手段とを備えることを特徴とする。

【0009】請求項 1 に記載の電子現金システムにおいては、口座管理装置が、利用者を識別する情報、および前払いの代金を基にした利用者の利用金額を記憶し、決済処理装置が、支払機関に決済を指示し、制御装置が、利用者を識別する情報、および決済処理装置の公開鍵で暗号化された利用者の支払機関の口座番号を管理し、利用者を特定する情報を基に、口座管理装置が記憶する利用者の前払いの残高の変更を指示し、支払い機関の口座番号を基に、決済処理装置に決済の実行を指示する。

【0010】

【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但

し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【0011】すなわち、請求項1に記載の電子現金システムは、口座管理装置（例えば、図1の仮想銀行4）が、利用者を特定する情報、および前払いの代金を基にした利用者の利用金額を記憶する記憶手段（例えば、図1の口座管理部45）を備え、決済処理装置（例えば、図1の精算所5）が、支払機関に決済を指示する決済指示手段（例えば、図1の精算部55）を備え、制御装置（例えば、図1のセンター3）が、利用者を特定する情報、および決済処理装置の公開鍵で暗号化された利用者の支払機関の口座番号を管理する管理手段（例えば、図1のユーザ管理部35）と、管理手段が管理する利用者を特定する情報を基に、口座管理装置の記憶手段が記憶する利用者の前払いの残高の変更を指示する残高変更指示手段（例えば、図1の通信部37）と、管理手段が管理する支払い機関の口座番号を基に、決済処理装置の決済指示手段に決済の実行を指示する決済実行指示手段（例えば、図1の通信部37）とを備えることを特徴とする。

【0012】図1は、本発明を適用した電子現金システムの構成を表す図である。ユーザ機器1-1は、販売店2から、商品を購入し、またはサービスを受け、センター3、仮想銀行4、および精算所5を介して、販売店2に代金を支払う。ユーザ機器1-2は、販売店2から、商品を購入し、またはサービスを受け、センター3、仮想銀行4、および精算所5を介して、販売店2に代金を支払う。販売店2は、ユーザ機器1-1または1-2に商品またはサービスを提供し、センター3、仮想銀行4、および精算所5を介して、ユーザ機器1-1またはユーザ機器1-2から代金を受け取る。センター3は、ユーザ機器1-1、ユーザ機器1-2、および販売店2の所定のデータを記憶し、ユーザ機器1-1、ユーザ機器1-2、および販売店2の決済処理を精算所5に実行させる。仮想銀行4は、電子マネーを発行する機関であり、電子マネーの発行単位（ユーザ機器1-1または1-2並びに販売店2）のIDを発行し、IDに対応する残高、または売り上げ金額などを管理する。精算所5は、銀行8またはカード会社7に対して、ユーザ機器1-1または1-2並びに販売店2の口座毎またはカード番号毎に、出金または入金の手続を実行する。認証局6は、ユーザ機器1-1乃至精算所5の要求に対応し、所定のデータを含んだ証明書を発行する。

【0013】ユーザ機器1-1の相互認証部11-1は、ユーザ機器1-2、販売店2、センター3、または認証局6と、後述する処理で相互認証する。記憶部12-1は、耐タンパー性を有する素子から構成され、電子マネーのユーザID、残高、および未精算金額を記憶する。暗号化部13-1は、ユーザ機器1-2、販売店2、またはセンター3に送信する、購入金額、購入品情

報、および電子マネーのユーザIDなどの所定のデータを暗号化する。復号部14-1は、ユーザ機器1-2、販売店2、センター3、または認証局6から受信する、ユーザID、金額、および残高などの暗号化された情報を復号する。署名部15-1は、ユーザ機器1-2、販売店2、センター3、または認証局6に送信する、購入金額、購入品情報、および電子マネーのユーザIDなどの所定のデータにハッシュ関数を適用してハッシュ値を算出し、所定の鍵で暗号化し、署名を作成する。署名部15-1はまた、ユーザ機器1-2、販売店2、センター3、または認証局6から受信する、データおよびデータに付された署名を検査し、改竄がなかったか否か判定する。通信部16-1は、ユーザ機器1-2、販売店2、センター3、または認証局6に所定のデータを送信し、ユーザ機器1-2、販売店2、センター3、または認証局6から送信されたデータを受信する。

【0014】ユーザ機器1-2の相互認証部11-2、記憶部12-2、暗号化部13-2、復号部14-2、署名部15-2、および通信部16-2は、ユーザ機器1-1の相互認証部11-1、記憶部12-1、暗号化部13-1、復号部14-1、署名部15-1、および通信部16-1と同様であり、その説明は省略する。なお、以下、特に区別する必要が無いときは、ユーザ機器1-1、ユーザ機器1-2を、単に、ユーザ機器1と称する。

【0015】販売店2の相互認証部21、センター3の相互認証部31、仮想銀行4の相互認証部41、および精算所5の相互認証部51は、ユーザ機器1-1の相互認証部11-1と同様の処理を行うのでその説明は省略する。

【0016】販売店2の暗号化部23、センター3の暗号化部32、仮想銀行4の暗号化部42、および精算所5の暗号化部52は、ユーザ機器1-1の暗号化部13-1と同様の処理を行うのでその説明は省略する。

【0017】販売店2の復号部24、センター3の復号部33、仮想銀行4の復号部43、および精算所5の復号部53は、ユーザ機器1-1の復号部14-1と同様の処理を行うのでその説明は省略する。

【0018】販売店2の署名部25、センター3の署名部34、仮想銀行4の署名部44、および精算所5の署名部54は、ユーザ機器1-1の署名部15-1と同様の処理を行うのでその説明は省略する。

【0019】販売店2の通信部26、センター3の通信部37、仮想銀行4の通信部46、および精算所5の通信部56は、ユーザ機器1-1の通信部16-1と同様の処理を行うのでその説明は省略する。

【0020】販売店2の記憶部22は、耐タンパー性を有する素子から構成され、販売店ID、および売り上げ金額などを記憶する。

【0021】センター3のユーザ管理部35は、ユーザ

IDに対応するユーザの公開鍵 K_{pu} 、および精算所5の公開鍵 K_{pg} で暗号化したユーザのクレジットカード番号を記憶し、管理する。センター3の販売店管理部36は、販売店IDに対応する販売店2の公開鍵 K_{pm} 、および精算所5の公開鍵 K_{pg} で暗号化した販売店2の口座番号を記憶し、管理する。

【0022】仮想銀行4の口座管理部45は、ユーザIDに対応するユーザの電子現金の残高、および販売店IDに対応する販売店2の売り上げ金額を記憶する。

【0023】精算所5の精算部55は、ユーザ機器1-1または1-2並びに販売店2の口座毎に、銀行8またはカード会社7に対して、出金または入金の手続を指示する。

【0024】ユーザ機器1が、仮想銀行4に初めて入金し、ユーザIDを登録するときの処理を、図2のフローチャートを用いて説明する。ステップS11において、ユーザ機器1の通信部16は、認証局6に個人情報、口座情報、およびユーザ機器1の公開鍵 K_{pu} を送信する。認証局6は、ユーザ機器1の通信部16が送信したデータを受信する。ステップS12において、認証局6は、受信した個人情報、口座情報、およびユーザ機器1の公開鍵 K_{pu} に所定のハッシュ関数を適用し、得られたハッシュ値を認証局6の秘密鍵 K_{sc} で暗号化して署名を作成し、個人情報、口座情報、およびユーザ機器1の公開鍵 K_{pu} に付加して証明書を作成し、ユーザ機器1に送信する。ユーザ機器1の通信部16は、認証局6が送信したデータを受信する。

【0025】署名は、データまたは証明書に付け、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値を取り、これを公開鍵暗号の秘密鍵で暗号化して作成される。

【0026】ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

【0027】署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数とし

ては、MD4、MD5、SHA-1などが用いられる。

【0028】次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

【0029】公開鍵暗号の中で代表的なRSA（Rivest-Shamir-Adleman）暗号を、簡単に説明する。まず、2つの十分に大きな素数である p および q を求め、さらに p と q の積である n を求める。 $(p-1)$ と $(q-1)$ の最小公倍数 L を算出し、更に、3以上 L 未満で、かつ、 L と互いに素な数 e を求める（すなわち、 e と L を共通に割り切れる数は、1のみである）。

【0030】次に、 L を法とする乗算に関する e の乗法逆元 d を求める。すなわち、 d 、 e 、および L の間には、 $ed=1 \bmod L$ が成立し、 d はユークリッドの互除法で算出できる。このとき、 n と e が公開鍵とされ、 p 、 q 、および d が、秘密鍵とされる。

【0031】暗号文 C は、平文 M から、式（1）の処理で算出される。

$$C=M^e \bmod n \quad (1)$$

【0032】暗号文 C は、式（2）の処理で平文 M に、復号される。

$$M=C^d \bmod n \quad (2)$$

【0033】証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式（3）が成立するからである。

$$M=C^d=(M^e)^d=M^{ed} \bmod n \quad (3)$$

【0034】秘密鍵 p と q を知っているならば、公開鍵 e から秘密鍵 d は算出できるが、公開鍵 n の素因数分解が計算量的に困難な程度に公開鍵 n の桁数を大きくすれば、公開鍵 n を知るだけでは、公開鍵 e から秘密鍵 d は計算できず、復号できない。以上のように、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【0035】また、公開鍵暗号の他の例である楕円曲線暗号についても、簡単に説明する。楕円曲線 $y^2=x^3+ax+b$ 上の、ある点を B とする。楕円曲線上の点の加算を定義し、 nB は、 B を n 回加算した結果を表す。同様に、減算も定義する。 B と nB から n を算出することは、困難であることが証明されている。 B と nB を公開鍵とし、 n を秘密鍵とする。乱数 r を用いて、暗号文 $C1$ および $C2$ は、平文 M から、公開鍵で式（4）および式（5）の処理で算出される。

$$C1=M+rnB \quad (4)$$

$$C2=rB \quad (5)$$

【0036】暗号文 $C1$ および $C2$ は、式（6）の処理で平

文Mに、復号される。

$M=C1-nC2$ (6)

【0037】復号できるのは、秘密鍵 n を有するものだけである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【0038】ステップS13において、ユーザ機器1の相互認証部11は、センター3の相互認証部31と、相互認証し、後述する乱数の接続 $R2 \parallel R3$ をセンター3とユーザ機器1の間の一時的鍵 $Ktsu$ として共有する。相互認証の手続については、図3のフローチャートを用いて、後述する。ステップS14において、ユーザ機器1の暗号化部13は、精算所5の公開鍵 $Kppg$ でユーザの予め記憶しているクレジットカード番号を暗号化し、署名部15は、ユーザ機器により設定された電子現金発行金額に署名を付す。ユーザ機器1の暗号化部13は、暗号化されたクレジットカード番号および署名を付された電子現金発行金額を一時的鍵 $Ktsu$ で暗号化し、通信部16は、精算所5の公開鍵 $Kppg$ で暗号化され、一時的鍵 $Ktsu$ で暗号化されたクレジットカード番号、および署名を付され、一時的鍵 $Ktsu$ で暗号化された電子現金発行金額をセンター3に送信する。センター3の通信部37は、ユーザ機器1から送信された、クレジットカード番号、および電子現金発行金額を受信する。

【0039】ステップS15において、センター3の復号部33は、一時的鍵 $Ktsu$ で暗号化されたクレジットカード番号および電子現金発行金額を復号し、署名部34は、電子現金発行金額に付された署名を、後述する相互認証で得られたユーザ機器1の証明書に含まれるユーザ機器の公開鍵 Kpu で、復号部33に復号させ得られた値と、一時的鍵 $Ktsu$ で復号した電子現金発行金額にハッシュ関数を適用して得られたハッシュ値とを比較し、同一であれば電子現金発行金額が改竄されていないと判定する。電子現金発行金額が改竄されていると判定された場合、処理は終了する。電子現金発行金額が改竄されていない場合、ステップS16に進み、センター3の相互認証部31は、精算所5の相互認証部51と相互認証し、センター3と精算所5の間の一時的鍵 $Ktsp$ を共有する。相互認証の手続については、図3のフローチャートを用いて、後述する。ステップS17において、センター3の署名部34は、電子現金発行金額に署名を付し、暗号化部32は、ユーザ機器1の証明書、精算所5の公開鍵 $Kppg$ で暗号化されたクレジットカード番号、並びにセンター3の署名およびユーザ機器1の署名を付した電子現金発行金額を一時的鍵 $Ktsp$ で暗号化し、通信部37は、暗号化されたデータを精算所5に送信する。精算所5の通信部56は、センター3から送信されたデータを受信する。

【0040】ステップS18において、精算所5の復号

部53は、センター3から受信したデータを一時的鍵 $Ktsp$ で復号し、精算所5の署名部54は、電子現金発行金額に付されたセンター3の署名およびユーザ機器1の署名を検証し、電子現金発行金額に改竄がないことを確認する。署名の検証の処理は、ステップS15における場合と同様であるので、その説明は省略する。署名部34が電子現金発行金額の改竄を発見した場合、処理は終了する。電子現金発行金額が改竄されていない場合、ステップS19に進み、署名部54は、受信したクレジットカード番号にハッシュ関数を適用してハッシュ値を算出し、証明書にあるハッシュ値と一致するかを検証し、クレジットカード番号に改竄がないことを確認する。署名部34がクレジットカード番号の改竄を発見した場合、処理は終了する。クレジットカード番号が改竄されていない場合、ステップS20に進み、精算部55は、通信部56を介して、クレジットカード会社7に、与信および引き落とし命令を送付する。

【0041】ステップS21において、署名部54は、ステップS18およびステップS19の検証結果並びにステップS20の処理結果に署名を付し、暗号化部52は、署名を付した検証結果および処理結果を暗号化し、通信部56は、暗号化した検証結果および処理結果をセンター3に送信する。センター3の通信部37は、精算所5が送信した検証結果および処理結果を受信し、復号部33は、精算所5から受信した検証結果および処理結果を復号する。受信した検証結果が不正があったことを示し、および処理結果が正常に終了しなかったことを示している場合、処理は終了する。

【0042】ステップS21で受信した検証結果が不正がないことを示し、および処理結果が正常に終了したことを示している場合、ステップS22において、センター3の相互認証部31は、仮想銀行4の相互認証部41と相互認証し、センター3と仮想銀行4の間で一時的鍵 $Ktsb$ を共有する。相互認証の手続については、図3のフローチャートを用いて、後述する。ステップS23において、暗号化部32は、ユーザ機器1の証明書、並びにステップS17で作成した、センター3の署名およびユーザ機器1の署名を付した電子現金発行金額を一時的鍵 $Ktsb$ で暗号化し、通信部37は、暗号化された、ユーザ機器1の証明書および電子現金発行金額を仮想銀行4に送信する。仮想銀行4の通信部46は、センター3から送信されたユーザ機器1の証明書および電子現金発行金額を受信する。

【0043】ステップS24において、仮想銀行4の復号部43は、センター3から受信したユーザ機器1の証明書および電子現金発行金額を一時的鍵 $Ktsb$ で復号し、署名部44は、電子現金発行金額に付されたセンター3の署名およびユーザ機器1の署名を検証し、電子現金発行金額に改竄がないことを確認する。署名の検証の処理は、ステップS15における場合と同様であるので、そ

の説明は省略する。署名部44が電子現金発行金額の改竄を発見した場合、処理は終了する。電子現金発行金額が改竄されていない場合、ステップS25において、仮想銀行4の口座管理部45は、ユーザIDを生成し、ユーザIDに対応させ、電子現金発行金額を記憶する。ステップS26において、署名部44は、ユーザIDに署名を付して、暗号化部42は、ユーザIDを一時鍵K_{tsb}で暗号化し、通信部46は、センター3に暗号化したユーザIDを送信する。センター3の通信部37は、仮想銀行4が送信したユーザIDを受信する。

【0044】ステップS27において、センター3の復号部33は、仮想銀行4が送信したユーザIDを一時鍵K_{tsb}で復号し、ユーザ機器管理部35は、復号したユーザID、ステップS13で受信したユーザ機器の公開鍵K_{pu}、およびステップS14で受信した精算所5の公開鍵K_{pg}で暗号化したクレジットカード番号の組を記憶し、管理する。ステップS28において、センター3の署名部34は、ユーザIDに署名を付して、暗号化部32は、一時鍵K_{tsu}でユーザIDを暗号化し、通信部37は、暗号化したユーザIDをユーザ機器に送信する。ユーザ機器1の通信部16は、センター3が送信したユーザIDを受信する。

【0045】ステップS29において、ユーザ機器1の復号部14は、受信したユーザIDを一時鍵K_{tsu}で復号し、記憶部12は、ステップS28で受信したユーザIDおよびステップS14で送信した電子現金発行金額を電子現金残高として記憶する。

【0046】このように、ユーザ機器1は、初めての入金で、仮想銀行4に、ユーザIDが登録され、ユーザIDと対応して先払いした金額と同額の電子現金発行金額が記憶される。

【0047】図2のステップS13における、公開鍵暗号である、160ビット長の楕円曲線暗号を用いる、ユーザ機器1の相互認証部11とセンター1の相互認証部31との相互認証の処理を、図3のフローチャートを用いて説明する。ステップS41において、ユーザ機器1の相互認証部11は、64ビットの乱数R1を生成する。ステップS42において、ユーザ機器1の相互認証部11は、自分自身の公開鍵K_{pu}を含む証明書（認証局6からステップS12で取得したもの）と、乱数R1をセンター3の相互認証部31に送信する。

【0048】ステップS43において、センター3の相互認証部31は、受信した証明書の署名（認証局6の秘密鍵K_{sca}で暗号化されている）を、予め取得しておいた認証局の公開鍵K_{pca}で復号し、ユーザ機器1の公開鍵K_{pu}とユーザ機器1の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているユーザ機器1の公開鍵K_{pu}およびユーザ機器1の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号し

て得られた公開鍵K_{pu}およびユーザ機器1の名前のハッシュ値は、平文のまま証明書に格納されていたユーザ機器1の公開鍵K_{pu}およびユーザ機器1の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵K_{pu}が改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なユーザ機器でないことになる。この時処理は終了される。

【0049】適正な認証結果が得られたとき、ステップS44において、センター3の相互認証部31は、64ビットの乱数R2を生成する。ステップS45において、センター3の相互認証部31は、乱数R1および乱数R2の接続R1 || R2を生成する。ステップS46において、センター3の相互認証部31は、接続R1 || R2を自分自身の秘密鍵K_{sec}で暗号化する。ステップS47において、センター3の相互認証部31は、接続R1 || R2を、ステップS43で取得したユーザ機器1の公開鍵K_{pu}で暗号化する。ステップS48において、センター3の相互認証部31は、秘密鍵K_{sec}で暗号化された接続R1 || R2、公開鍵K_{pu}で暗号化された接続R1 || R2、および自分自身の公開鍵K_{pesc}を含む証明書（認証局から予め取得しておいたもの）をユーザ機器1の相互認証部11に送信する。

【0050】ステップS49において、ユーザ機器1の相互認証部11は、受信した証明書の署名を予め取得しておいた認証局の公開鍵K_{pca}で復号し、正しければ証明書から公開鍵K_{pesc}を取り出す。この場合の処理は、ステップS43における場合と同様であるので、その説明は省略する。ステップS50において、ユーザ機器1の相互認証部11は、センター3の秘密鍵K_{sec}で暗号化されている接続R1 || R2を、ステップS49で取得した公開鍵K_{pesc}で復号する。ステップS51において、ユーザ機器1の相互認証部11は、自分自身の公開鍵K_{pu}で暗号化されている接続R1 || R2を、自分自身の秘密鍵K_{su}で復号する。ステップS52において、ユーザ機器1の相互認証部11は、ステップS50で復号された接続R1 || R2と、ステップS51で復号された接続R1 || R2を比較し、一致すればセンター3を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

【0051】適正な認証結果が得られたとき、ステップS53において、ユーザ機器1の相互認証部11は、64ビットの乱数R3を生成する。ステップS54において、ユーザ機器1の相互認証部11は、ステップS50で取得した乱数R2および生成した乱数R3の接続R2 || R3を生成する。ステップS55において、ユーザ機器1の相互認証部11は、接続R2 || R3を、ステップS49で取得した公開鍵K_{pesc}で暗号化する。ステップS56において、ユーザ機器1の相互認証部11

は、暗号化した接続 $R2 \parallel R3$ をセンター3の相互認証部31に送信する。

【0052】ステップS57において、センター3の相互認証部31は、暗号化された接続 $R2 \parallel R3$ を自分自身の秘密鍵 K_{esc} で復号する。ステップS58において、センター3の相互認証部31は、復号した乱数 $R2$ が、ステップS44で生成した乱数 $R2$ (暗号化する前の乱数 $R2$) と一致すれば、ユーザ機器1を適正なユーザ機器として認証し、一致しなければ、不適正なユーザ機器として、処理を終了する。

【0053】以上のように、センター3の相互認証部31とユーザ機器1の相互認証部11は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵として利用される。

【0054】ユーザ機器1が、仮想銀行4に2回目以降に入金するときの処理を、図4のフローチャートを用いて説明する。ステップS71において、ユーザ機器1の相互認証部11は、センター3の相互認証部31と、相互認証し、センター3とユーザ機器1の間の一時鍵 K_{tsu} を共有する。相互認証の手続は、図3で説明したものと同様であり、その説明は省略する。ステップS72において、ユーザ機器1の署名部15は、ユーザIDに署名を付し、電子現金発行金額に署名を付す。ユーザ機器1の暗号化部13は、署名を付されたユーザIDおよび署名を付された電子現金発行金額を一時鍵 K_{tsu} で暗号化し、通信部16は、一時鍵 K_{tsu} で暗号化されたユーザIDおよび電子現金発行金額をセンター3に送信する。センター3の通信部37は、ユーザ機器1から送信された、一時鍵 K_{tsu} で暗号化されたユーザIDおよび電子現金発行金額を受信する。

【0055】ステップS73において、センター3の復号部33は、一時鍵 K_{tsu} で暗号化されたユーザIDおよび電子現金発行金額を一時鍵 K_{tsu} で復号し、署名部34は、復号して得られた、電子現金発行金額に付された署名を検証し、電子現金発行金額が改竄されていないことを確認する。署名の検証は、図2のステップS15で説明した処理と同様なので、その説明は省略する。署名部34が電子現金発行金額の改竄を発見した場合、処理は終了する。電子現金発行金額が改竄されていない場合、ステップS74に進み、センター3のユーザ管理部35は、ユーザIDに対応する、図2のステップS27で記憶した精算所5の公開鍵 K_{ppg} で暗号化したクレジットカード番号を求める。

【0056】ステップS75乃至ステップS81は、図2のステップS16乃至ステップS22とそれぞれ同様であるので、その説明は省略する。

【0057】ステップS82において、センター3の署名部34は、ステップS72で受信したユーザ機器の署名を付したユーザIDに署名を付し、ステップS72で受信したユーザ機器の署名を付した電子現金発行金額に署

名を付し、暗号化部32は、一時鍵 K_{tsb} でユーザIDおよび電子現金発行金額を暗号化し、通信部37は、暗号化したユーザIDおよび電子現金発行金額を仮想銀行4に送信する。仮想銀行4の通信部46は、センター3が送信したユーザIDおよび電子現金発行金額を受信する。

【0058】ステップS83において、仮想銀行4の復号部43は、ステップS82で受信したユーザIDおよび電子現金発行金額を一時鍵 K_{tsb} で復号し、署名部44は、電子現金発行金額に付されたセンター3の署名およびユーザ機器1の署名を検証し、電子現金発行金額に改竄がないことを確認する。署名の検証は、図2のステップS15で説明した処理と同様なので、その説明は省略する。署名部44が電子現金発行金額の改竄を発見した場合、処理は終了する。電子現金発行金額が改竄されていない場合、ステップS84において、口座管理部45は、ユーザIDに対応する電子現金の金額に、今回の電子現金発行金額を加算する。

【0059】ステップS85乃至ステップS87は、図2のステップS26乃至ステップS28の処理とそれぞれ同様であり、その説明は省略する。

【0060】ステップS88において、ユーザ機器1の記憶部12は、記憶部12が記憶する電子現金残高に、ステップS72で送信した電子現金発行金額を加算し、記憶する。

【0061】このように、ユーザ機器1は、仮想銀行4に2回目以降も電子現金を入金することができる。

【0062】次に、販売店2がセンター3および仮想銀行4に登録する処理を、図5のフローチャートを用いて説明する。ステップS91において、販売店2の通信部26は、認証局6に販売店情報、口座情報、および販売店2の公開鍵 K_{pm} を送信する。認証局6は、販売店2の通信部26が送信したデータを受信する。ステップS92において、認証局6は、受信した販売店情報、口座情報、および販売店2の公開鍵 K_{pm} に所定のハッシュ関数を適用し、得られたハッシュ値を認証局6の秘密鍵 K_{sca} で暗号化して署名を作成し、販売店情報、口座情報、および販売店2の公開鍵 K_{pm} に付加して証明書を作成し、販売店2に送信する。販売店2の通信部26は、認証局6が送信したデータを受信する。

【0063】ステップS93において、販売店2の相互認証部21は、センター3の相互認証部31と、相互認証し、販売店2およびセンター3は、図3のステップS54およびステップS57の乱数の接続 $R2 \parallel R3$ を一時鍵 K_{tsm} として共有する。相互認証の手続は、図3の処理と同様であるので説明は省略する。ステップS94において、販売店2の暗号化部23は、精算所5の公開鍵 K_{ppg} で予め記憶している販売店2の口座番号を暗号化する。販売店2の暗号化部23は、精算所5の公開鍵 K_{ppg} で暗号化された口座番号を一時鍵 K_{tsm} で更に暗号化し、販売店2の証明書も一時鍵 K_{tsm} で

暗号化する。通信部26は、一時鍵K t s mで暗号化された口座番号および販売店2の証明書をセンター3に送信する。センター3の通信部37は、販売店2から送信された、一時鍵K t s mで暗号化された口座番号および証明書を受信し、復号部33は、一時鍵K t s mで暗号化された口座番号および証明書を復号する。

【0064】ステップS95に進み、センター3の相互認証部31は、精算所5の相互認証部51と相互認証し、センター3の相互認証部31および精算所5の相互認証部51は、図3のステップS54およびステップS57の乱数の接続R2 || R3を一時鍵K t s pとして共有する。相互認証の手続は、図3の処理と同様であるので説明は省略する。ステップS96において、センター3の署名部34は、販売店2の口座番号に署名を付し、暗号化部32は、販売店2の証明書、およびセンター3の署名を付され、精算所5の公開鍵K p p gで暗号化された口座番号を、一時鍵K t s pで更に暗号化し、通信部37は、一時鍵K t s pで暗号化されたデータを精算所5に送信する。精算所5の通信部56は、センター3から送信されたデータを受信する。

【0065】ステップS97において、精算所5の復号部53は、センター3から受信したデータを一時鍵K t s pで復号し、精算所5の署名部54は、証明書に付された認証局6の署名を検証し、証明書に改竄がないことを確認する。署名部34が証明書の改竄を発見した場合、処理は終了する。証明書が改竄されていない場合、ステップS98に進み、署名部54は、受信した口座番号にハッシュ関数を適用してハッシュ値を算出し、証明書にあるハッシュ値と一致するかを検証し、口座番号に改竄がないことを確認する。署名部34が口座番号の改竄を発見した場合、処理は終了する。口座番号に改竄がない場合、ステップS99において、署名部54は、ステップS98およびステップS98の検証結果に署名を付し、暗号化部52は、一時鍵K t s pで署名を付した検証結果を暗号化し、通信部56は、一時鍵K t s pで暗号化した検証結果をセンター3に送信する。センター3の通信部37は、精算所5が送信した検証結果を受信し、復号部33は、精算所5から受信した検証結果を一時鍵K t s pで復号する。

【0066】ステップS100において、センター3の相互認証部31は、仮想銀行4の相互認証部41と相互認証し、センター3および仮想銀行4は、図3のステップS54およびステップS57の乱数の接続R2 || R3を一時鍵K t s bとして共有する。相互認証の手続は、図3の処理と同様であるので説明は省略する。ステップS101において、センター3の署名部34は、証明書にセンター3の署名を付し、暗号化部32は、センター3の署名を付した販売店2の証明書を一時鍵K t s bで暗号化し、通信部37は、一時鍵K t s bで暗号化された販売店2の証明書を仮想銀行4に送信する。仮想銀行

4の通信部46は、センター3から送信された販売店2の証明書を受信する。

【0067】ステップS102において、仮想銀行4の復号部43は、センター3から受信した販売店2の証明書を一時鍵K t s bで復号し、署名部44は、販売店2の証明書に付されたセンター3の署名および販売店2の証明書に含まれる認証局6の署名を検証し、販売店2の証明書に改竄がないことを確認する。販売店2の証明書に改竄が発見された場合、処理は終了する。販売店2の証明書に改竄がない場合、ステップS103において、仮想銀行4の口座管理部45は、販売店IDを生成し、販売店IDに対応する売り上げ金額を記憶する。

【0068】ステップS104乃至ステップS106の処理は、図2のステップS26乃至ステップS28の処理にそれぞれ同様の処理であるのでその説明は、省略する。

【0069】ステップS107において、販売店2の復号部24は、受信した販売店IDを復号し、記憶部22は、ステップS106で受信した販売店IDを記憶する。

【0070】このように、販売店2は、センター3および仮想銀行4に登録し、販売店IDを記憶する。

【0071】次に、ユーザ機器1-2からユーザ機器1-1への電子現金の移動を、図6のフローチャートを用いて説明する。ステップS121において、ユーザ機器1-2の相互認証部11-2は、ユーザ機器1-1の相互認証部11-1と、相互認証し、ユーザ機器1-2およびユーザ機器1-1は、図3のステップS54およびステップS57の乱数の接続R2 || R3を一時鍵K t u uとして共有する。相互認証の手続は、図3の処理と同様であるので説明は省略する。ステップS122において、ユーザ機器1-2の署名部15-2は、ユーザにより設定された移動する金額を示すデータに署名を付し、暗号化部13-2は、移動する金額を示すデータを一時鍵K t u uで暗号化する。ユーザ機器1-2の通信部16-2は、一時鍵K t u uで暗号化された金額を示すデータをユーザ機器1-1の通信部16-1に送信する。ユーザ機器1-1の通信部16-1は、一時鍵K t u uで暗号化された金額を示すデータを受信する。

【0072】ステップS123において、ユーザ機器1-1の復号部14-1は、暗号化された金額を示すデータを一時鍵K t u uで復号し、記憶部12-1は、記憶している未精算金額に、移動する金額を加算し、記憶する。未精算金額とは、他のユーザ機器1から移動し、受け取った金額の総額を言う。ステップS124において、ユーザ機器1-1の署名部15-1は、移動する金額を示すデータに署名を付し、暗号化部13-1は、移動する金額を示すデータを一時鍵K t u uで暗号化する。ユーザ機器1-1の通信部16-1は、暗号化した金額を示すデータをユーザ機器1-2の通信部16-2に送信する。ユーザ機器1-2の通信部16-2は、暗

号化した金額を示すデータを受信する。

【0073】ステップS125において、ユーザ機器1-2の復号部14-2は、暗号化した金額を示すデータを一時鍵K_{tuu}で復号し、記憶部12-2は、記憶している未精算金額から、復号した得られた、移動する金額を減じ、記憶する。ステップS126において、署名部15-2は、電子現金の移動の終了を示すデータに署名を付し、暗号化部13-2は、署名を付した電子現金の移動の終了を示すデータを一時鍵K_{tuu}で暗号化し、通信部16-2は、暗号化された電子現金の移動の終了を示すデータをユーザ機器1-1の通信部16-1に送信する。ユーザ機器1-1の通信部16-1は、一時鍵K_{tuu}で暗号化された電子現金の移動の終了を示すデータを受信し、処理は終了する。

【0074】以上のように、ユーザ機器1-2は、ユーザ機器1-1に電子現金を移動する。

【0075】図7は、ユーザ機器1-2からユーザ機器1-1への電子現金の移動の他の処理を説明するフローチャートである。ステップS131において、ユーザ機器1-2の相互認証部11-2は、ユーザ機器1-1の相互認証部11-1と、相互認証し、ユーザ機器1-2およびユーザ機器1-1は、図3のステップS54およびステップS57の乱数の接続R2∥R3を一時鍵K_{tuu}として共有する。相互認証の手続は、図3の処理と同様であるので説明は省略する。ステップS132において、ユーザ機器1-2の署名部15-2は、ユーザにより設定された移動する金額を示すデータに署名を付し、暗号化部13-2は、センター3の公開鍵K_{pesc}でユーザ機器1-2のユーザIDを暗号化し、更に移動する金額を示すデータおよびセンター3の公開鍵K_{pesc}で暗号化したユーザ機器1-2のユーザIDを一時鍵K_{tuu}で暗号化する。ユーザ機器1-2の通信部16-2は、一時鍵K_{tuu}で暗号化した金額を示すデータおよびユーザ機器1-2のユーザIDを、ユーザ機器1-1の通信部16-1に送信する。ユーザ機器1-1の通信部16-1は、暗号化した金額を示すデータおよびユーザ機器1-2のユーザIDを受信する。

【0076】ステップS133において、ユーザ機器1-1の復号部14-1は、暗号化した金額を示すデータおよびユーザ機器1-2のユーザIDを一時鍵K_{tuu}で復号し、記憶部12-1は、記憶している未精算金額に、移動する金額を加算し、得られた金額およびセンター3の公開鍵K_{pesc}で暗号化したユーザ機器1-2のユーザIDを、記憶する。

【0077】ステップS134乃至ステップS136の処理は、図6のステップS124乃至ステップS126の処理とそれぞれ同様であり、その説明は省略する。

【0078】図7の処理により、ユーザ機器1-2は、ユーザ機器1-1に電子現金を移動し、ユーザ機器1-1は、移動し現金と共に、ユーザ機器1-2のユーザID

を記憶する。

【0079】次に、電子現金によるユーザ機器1から販売店2への支払いの処理を、図8のフローチャートを用いて説明する。ステップS151において、ユーザは、ユーザ機器1の記憶部12に記憶する電子現金の残高を確認し、購入金額に対して、不足している場合は、図4に示す処理を行い、必要な電子現金の額を記憶させる。ステップS152において、ユーザ機器1の相互認証部11は、販売店2の相互認証部21と、相互認証し、ユーザ機器1および販売店2は、図3のステップS54およびステップS57の乱数の接続R2∥R3を一時鍵K_{tum}として共有する。相互認証の手続は、図3の処理と同様であるので説明は省略する。

【0080】ステップS153において、ユーザ機器1の暗号化部13は、販売店2から購入する購入品の情報（ユーザ機器1の操作により、ユーザが指定した購入品の情報）を、予め記憶部12に記憶した販売店2の公開鍵K_{pm}で暗号化し、ユーザIDを、予め記憶部12に記憶したセンター3の公開鍵K_{pesc}で暗号化し、記憶部12に記憶した未精算金額を仮想銀行4の公開鍵K_{pvb}で暗号化する。

【0081】次に、ユーザ機器1の署名部15は、購入品に関する情報およびユーザIDに署名を付し、仮想銀行4の公開鍵K_{pvb}で暗号化した未精算金額に署名を付し、センター3の公開鍵K_{pesc}で暗号化したユーザIDに署名を付し、購入金額に署名を付す。ユーザ機器1の暗号化部13は、販売店2の公開鍵K_{pm}で暗号化した購入品に関する情報、センター3の公開鍵K_{pesc}で暗号化したユーザID、購入品に関する情報およびユーザIDに対する署名、署名を付した仮想銀行4の公開鍵K_{pvb}で暗号化した未精算金額、署名を付したセンター3の公開鍵K_{pesc}で暗号化したユーザID、並びに署名を付した購入金額を、一時鍵K_{tum}で更に暗号化する。ユーザ機器1の通信部16は、一時鍵K_{tum}で暗号化された、販売店2の公開鍵K_{pm}で暗号化した購入品に関する情報、センター3の公開鍵K_{pesc}で暗号化したユーザID、購入品に関する情報およびユーザIDに対する署名、署名を付した仮想銀行4の公開鍵K_{pvb}で暗号化した未精算金額、署名を付したセンター3の公開鍵K_{pesc}で暗号化したユーザID、並びに署名を付した購入金額を、販売店2の通信部26に送信し、販売店2の通信部26は、これらのデータを受信する。

【0082】ステップS154において、販売店2の復号部24は、ステップS153で受信した、販売店2の公開鍵K_{pm}で暗号化した購入品に関する情報、センター3の公開鍵K_{pesc}で暗号化したユーザID、購入品に関する情報およびユーザIDに対する署名、署名を付した仮想銀行4の公開鍵K_{pvb}で暗号化した未精算金額、署名を付したセンター3の公開鍵K_{pesc}で暗号化したユーザID、並びに署名を付した購入金額を、一時

鍵K t u mで復号する。署名部3 4は、購入品に関する情報およびユーザIDに対するユーザ機器1の署名を確認し、改竄があったかどうかを確認し、改竄があったと判定された場合、処理は、終了する。改竄がないと判定された場合、復号部2 4は、販売店2の公開鍵K p mで暗号化した購入品に関する情報を、販売店2の秘密鍵K s mで復号する。また、購入品に対する情報、金額より、購入品に対する金額の確認と、販売店2の公開鍵K p mで暗号化した購入品に関する情報、センター3の公開鍵K p e s cで暗号化したユーザID、購入品に関する情報およびユーザIDに対する署名より、ユーザID、購入品の組が正しいことを確認する。

【0083】ステップS155において、販売店2の相互認証部2 1は、センター3の相互認証部3 1と相互認証し、販売店2およびセンター3は、図3のステップS54およびステップS57の乱数の接続R2 || R3を一時鍵K t s mとして共有する。相互認証の手続は、図3の処理と同様であるので説明は省略する。

【0084】ステップS156において、販売店2の暗号化部2 3は、記憶部2 2に記憶している販売店2の販売店IDを、ステップS155で得られたセンター3の公開鍵K p e s cで暗号化し、署名部2 5は、センター3の公開鍵K p e s cで暗号化した販売店IDに署名を付し、ステップS154で復号した購入金額に対するユーザ機器1の署名に署名を付す。暗号化部3 2は、ステップ152で得られたユーザの証明書、センター3の公開鍵K p e s cで暗号化し、販売店の署名およびユーザ機器1の署名を付したユーザID、仮想銀行4の公開鍵K p v bで暗号化し、ユーザ機器1の署名を付した未精算金額、署名を付したセンター3の公開鍵K p e s cで暗号化した販売店ID、並びに署名を付した購入金額を、一時鍵K t s mで暗号化し、通信部2 6は、それらのデータをセンター3の通信部3 7に送信する。センター3の通信部3 7は、一時鍵K t s mで暗号化された、ステップ152で得られたユーザの証明書、センター3の公開鍵K p e s cで暗号化し、販売店の署名およびユーザ機器1の署名を付したユーザID、仮想銀行4の公開鍵K p v bで暗号化し、ユーザ機器1の署名を付した未精算金額、署名を付したセンター3の公開鍵K p e s cで暗号化した販売店ID、並びに署名を付した購入金額を受信する。

【0085】ステップS157において、センター3の復号部3 3は、ステップS156で受信した、ユーザの証明書、センター3の公開鍵K p e s cで暗号化した販売店の署名およびユーザ機器1の署名を付したユーザID、仮想銀行4の公開鍵K p v bで暗号化し、ユーザ機器1の署名を付した未精算金額、署名を付したセンター3の公開鍵K p e s cで暗号化した販売店ID、並びに署名を付した購入金額を一時鍵K t s mで復号する。署名部3 4は、購入金額へのユーザ機器1の署名および販売店2

の署名、ユーザIDに付した販売店の署名およびユーザ機器1の署名、並びに販売店IDへの販売店2の署名を検証し、購入金額、ユーザID、および販売店IDに改竄がないことを確認する。署名部3 4が購入金額、ユーザID、または販売店IDのいずれかに改竄を発見した場合、処理は終了する。購入金額、ユーザID、および販売店IDが改竄されていない場合、ステップS158において、センター3の相互認証部3 1は、仮想銀行4の相互認証部4 1と相互認証し、センター3および仮想銀行4は、図3のステップS54およびステップS57の乱数の接続R2 || R3を一時鍵K t s bとして共有する。相互認証の手続は、図3の処理と同様であるので説明は省略する。

【0086】ステップS159において、センター3の署名部3 4は、ユーザID、販売店ID、購入金額、仮想銀行4の公開鍵K p v bで暗号化した未精算金額に署名を付し、センター3の暗号化部3 2は、ユーザID、販売店ID、購入金額、仮想銀行の公開鍵K p v bで暗号化した未精算金額、および署名を一時鍵K t s bで暗号化し、通信部3 7は、暗号化したユーザID、販売店ID、購入金額、仮想銀行4の公開鍵K p v bで暗号化した未精算金額、および署名を、仮想銀行4の通信部4 6に送信する。仮想銀行4の通信部4 6は、暗号化したユーザID、販売店ID、購入金額、仮想銀行4の公開鍵K p v bで暗号化した未精算金額、および署名を、受信する。

【0087】ステップS160において、仮想銀行4の復号部4 3は、暗号化したユーザID、販売店ID、購入金額、仮想銀行4の公開鍵K p v bで暗号化した未精算金額、およびセンター3の署名を一時鍵K t s bで復号する。署名部4 4は、センター3の署名を検証し、ユーザID、販売店ID、購入金額、および仮想銀行4の公開鍵K p v bで暗号化した未精算金額に改竄がないことを確認する。署名部4 4が、改竄を発見した場合、処理は終了する。ユーザID、販売店ID、購入金額、および仮想銀行4の公開鍵K p v bで暗号化した未精算金額のいずれにも改竄がない場合、口座管理部4 5は、販売店IDに対応する売り上げ金額に購入金額を加算する。ステップS161において、口座管理部4 5は、ユーザIDに対応する残高から購入金額を減じ、ユーザIDに対応する残高に未精算金額を加算し、記憶する。

【0088】ステップS162において、仮想銀行4の暗号化部4 2は、ステップS161で記憶したユーザIDに対応する残高をユーザの公開鍵K p uで暗号化し、署名部4 4は、購入金額およびユーザの公開鍵K p uで暗号化したユーザIDに対応する残高に署名し、通信部4 6は、購入金額、ユーザの公開鍵K p uで暗号化したユーザIDに対応する残高、および署名をセンター3の通信部3 7に送信し、センター3の通信部3 7は、購入金額、ユーザの公開鍵K p uで暗号化したユーザIDに対応する残高、および署名を受信する。

【0089】ステップS163において、センター3の

復号部33は、購入金額、ユーザの公開鍵K_{pu}で暗号化したユーザIDに対応する残高、および仮想銀行4の署名を復号し、センター3の署名部34は、購入金額、ユーザの公開鍵K_{pu}で暗号化したユーザIDに対応する残高、および仮想銀行4の署名に、センター3の署名を付し、暗号化部32は、センター3の署名を付した、購入金額、ユーザの公開鍵K_{pu}で暗号化したユーザIDに対応する残高、および仮想銀行4の署名を一時鍵K_{t_{sm}}で暗号化する。通信部37は、販売店2の通信部26に、一時鍵K_{t_{sm}}で暗号化した、購入金額、ユーザの公開鍵K_{pu}で暗号化したユーザIDに対応する残高、仮想銀行4の署名、およびセンター3の署名を送信する。販売店2の通信部26は、これらのデータを受信する。

【0090】ステップS164において、販売店2の復号部24は、受信した購入金額、ユーザの公開鍵K_{pu}で暗号化したユーザIDに対応する残高、仮想銀行4の署名、およびセンター3の署名を一時鍵K_{t_{sm}}で復号し、署名部25は、仮想銀行4の署名、およびセンター3の署名を検証し、受信した購入金額、およびユーザの公開鍵K_{pu}で暗号化したユーザIDに対応する残高に改竄がないことを確認する。署名部25が、改竄を発見した場合、処理は終了する。受信した購入金額、およびユーザの公開鍵K_{pu}で暗号化したユーザIDに対応する残高のいずれにも改竄がない場合、ステップS165に進み、署名部25は、購入金額、ユーザの公開鍵K_{pu}で暗号化したユーザIDに対応する残高、仮想銀行4の署名、およびセンター3の署名に販売店2の署名を付し、暗号化部23は、一時鍵K_{t_{sm}}で購入金額、ユーザの公開鍵K_{pu}で暗号化したユーザIDに対応する残高、仮想銀行4の署名、センター3の署名、および販売店2の署名を暗号化し、通信部26は、暗号化された購入金額、ユーザの公開鍵K_{pu}で暗号化したユーザIDに対応する残高、仮想銀行4の署名、センター3の署名、および販売店2の署名をユーザ機器1の通信部16に送信する。ユーザ機器1の通信部16は、購入金額、ユーザの公開鍵K_{pu}で暗号化したユーザIDに対応する残高、仮想銀行4の署名、センター3の署名、および販売店2の署名を受信する。

【0091】ステップS166において、ユーザ機器1の復号部14は、受信した購入金額、ユーザの公開鍵K_{pu}で暗号化したユーザIDに対応する残高、仮想銀行4の署名、センター3の署名、および販売店2の署名を一時鍵K_{t_{sm}}で復号し、署名部15は、仮想銀行4の署名、センター3の署名、および販売店2の署名を検証し、受信した購入金額、およびユーザの公開鍵K_{pu}で暗号化したユーザIDに対応する残高に改竄がないことを確認する。署名部15が、改竄を発見した場合、処理は終了する。受信した購入金額、およびユーザの公開鍵K_{pu}で暗号化したユーザIDに対応する残高のいずれにも改竄がない場合、記憶部12は、受信した残高が、処理

開始前から記憶部12に記憶する残高より購入金額を減じ、ステップS153で送信した未精算金額を加えた金額と等しいかを確認し、受信した残高が、処理開始前から記憶部12に記憶する残高より購入金額を減じ、ステップS153で送信した未精算金額を加えた金額と等しい場合、残高を更新して記憶し、未精算金額を0とし、処理は終了する。受信した残高が、処理開始前から記憶部12に記憶する残高より購入金額を減じ、ステップS153で送信した未精算金額を加えた金額と等しくない場合、処理は終了する。

【0092】以上のように、ユーザ機器1は、仮想銀行4を介して、販売店2に支払いを行う。

【0093】図9のフローチャートを用いて、販売店2の口座への売上金の入金処理を説明する。ステップS181において、販売店2の相互認証部21は、センター3の相互認証部31と、相互認証し、販売店2およびセンター3は、図3のステップS54およびステップS57の乱数の接続R2 || R3を一時鍵K_{t_{sm}}として共有する。相互認証の手続は、図3の処理と同様であるので説明は省略する。ステップS182において、販売店2の暗号化部23は、一時鍵K_{t_{sm}}で、図5のステップS107で記憶部22に記憶している販売店2の販売店IDを暗号化する。販売店2の署名部25は、暗号化した販売店IDに署名を付し、暗号化部23は、販売店IDおよび署名を一時鍵K_{t_{sm}}で暗号化する。通信部26は、一時鍵K_{t_{sm}}で暗号化された販売店IDおよび署名をセンター3の通信部37に送信し、センター3の通信部37は、販売店IDおよび署名を受信する。

【0094】ステップS183において、センター3の復号部33は、一時鍵K_{t_{sm}}で暗号化された販売店IDおよび署名を復号し、署名部34は、復号して得られた、販売店IDに付された署名を検証し、販売店IDが改竄されていないことを確認する。販売店IDに改竄が発見されれば、処理は終了する。販売店IDに改竄が発見されない場合、ステップS184において、センター3の相互認証部31は、仮想銀行4の相互認証部41と相互認証し、センター3および仮想銀行4は、一時鍵K_{t_{sb}}を共有する。相互認証の手続は、図3の処理と同様であるので説明は省略する。ステップS185において、センター3の署名部34は、ステップS183で確認された販売店IDに署名を付し、暗号化部32は、販売店IDおよび署名を一時鍵K_{t_{sb}}で暗号化する。通信部37は、一時鍵K_{t_{sb}}で暗号化された販売店IDおよび署名を仮想銀行4の通信部46に送信し、仮想銀行4の通信部46は、販売店IDおよび署名を受信する。

【0095】ステップS186において、仮想銀行4の復号部43は、一時鍵K_{t_{sb}}で暗号化された販売店IDおよび署名を復号し、署名部44は、復号して得られた、販売店IDに付された署名を検証し、販売店IDが改竄されていないことを確認する。販売店IDに改竄が発見さ

れば、処理は終了する。販売店IDに改竄が発見されなければ、口座管理部45は、口座管理部45に記憶する販売店IDに対応する売り上げ金額をクリアする。ステップS187において、署名部44は、口座管理部45に記憶する販売店IDに対応する売り上げ金額（クリアする前の売り上げ金額）に署名を付し、暗号化部42は、売り上げ金額および署名を一時鍵Ktsbで暗号化する。通信部46は、一時鍵Ktsbで暗号化された売り上げ金額および署名をセンター3の通信部37に送信し、センター3の通信部37は、売り上げ金額および署名を受信する。

【0096】ステップS188において、センター3の相互認証部31は、精算所5の相互認証部51と相互認証し、センター3および精算所5は、一時鍵Ktspを共有する。相互認証の手続は、図3の処理と同様であるので説明は省略する。ステップS189において、センター3の署名部34は、ステップS187で仮想銀行4から受信した売り上げ金額に署名を付し、暗号化部32は、ステップS181の相互認証の処理で販売店2から受信した販売店の証明書、図5のステップ105で販売店管理部36に記憶した、精算所5の公開鍵Kpgで暗号化した販売店IDに対応する口座番号、およびセンター3の署名を付した売り上げ金額を一時鍵Ktspで暗号化する。通信部37は、一時鍵Ktspで暗号化した、販売店の証明書、販売店IDに対応する口座番号、および売り上げ金額を、精算所5の通信部56に送信する。精算所5の通信部56は、一時鍵Ktspで暗号化した、販売店の証明書、販売店IDに対応する口座番号、および売り上げ金額を受信する。

【0097】ステップS190において、精算所5の復号部53は、販売店の証明書、販売店IDに対応する口座番号、および売り上げ金額を復号し、署名部54は、復号した売り上げ金額に改竄がないことを確認し、改竄が発見されれば、処理は終了する。改竄が発見されなければ、精算部55は、売り上げ金額に相当する金額を販売店IDに対応する口座番号に入金する処理を、銀行に実行させる。ステップS191において、署名部54は、ステップS190の処理の結果を示すデータに署名を付し、通信部56は、入金処理の結果を示すデータおよび署名をセンター3の通信部37に送信する。センター3の通信部37は、入金処理の結果を示すデータおよび署名を受信する。

【0098】ステップS192において、センター3の復号部33は、入金処理の結果を示すデータおよび署名を復号し、署名部34は、入金処理の結果を示すデータに改竄がないことを確認し、改竄が発見されれば、処理は終了する。改竄が発見されなければ、署名部34は、入金処理の結果を示すデータに署名を付し、通信部37は、入金処理の結果を示すデータおよび署名を販売店2の通信部26に送信する。販売店2の通信部26は、入

金処理の結果を示すデータおよび署名を受信し、販売店2の復号部24は、入金処理の結果を示すデータおよび署名を復号し、署名部25は、入金処理の結果を示すデータに改竄がないことを確認し、記憶部22は、入金処理の結果を示すデータを記憶し、処理は終了する。

【0099】以上のように、販売店2の口座への売り上げ金の入金が処理される。

【0100】このように、各装置での利用者の識別をユーザIDで行う。個人情報各装置が把握しておらず、不正検出時には、センター3がユーザIDを基に精算所5の公開鍵Kpgで暗号化された口座情報を求め、精算所5に対して口座情報の開示を要求する。それを基に、認証局6、クレジットカード会社7、または銀行8に対して個人情報の特定を行う。その場合、どういうケースで各装置が情報を開示するかという制御ができ、またそれらを参照した履歴も管理できるため、不必要に個人情報が開示されることはない。

【0101】なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【0102】なお、上記したような処理を行うコンピュータプログラムをユーザ機器に提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【0103】

【発明の効果】請求項1に記載の電子現金システムによれば、口座管理装置が、利用者を識別する情報、および前払いの代金を基にした利用者の利用金額を記憶し、決済処理装置が、支払機関に決済を指示し、制御装置が、利用者を識別する情報、および決済処理装置の公開鍵で暗号化された利用者の支払機関の口座番号を管理し、利用者を特定する情報を基に、口座管理装置が記憶する利用者の前払いの残高の変更を指示し、支払い機関の口座番号を基に、決済処理装置に決済の実行を指示するようにしたので、利用者が特殊な装置を管理する必要がなく、安全に電子現金の利用ができ、個人の情報および個人の購入情報を各装置が不必要に把握できず、不正の検出が可能で、金銭の流通が管理できる。

【図面の簡単な説明】

【図1】本発明を適用した電子現金システムの構成を表す図である。

【図2】仮想銀行4に初めて入金し、ユーザIDを登録するときの処理を説明するフローチャートである。

【図3】相互認証の処理を説明するフローチャートである。

【図4】ユーザ機器1が、仮想銀行4に2回目以降に入金するときの処理を説明するフローチャートである。

【図5】販売店2がセンター3および仮想銀行4に登録する処理を説明するフローチャートである。

【図6】 ユーザ機器1-2からユーザ機器1-1への電子現金の移動する処理を説明するフローチャートである。

【図7】 ユーザ機器1-2からユーザ機器1-1への電子現金の移動する処理を説明するフローチャートである。

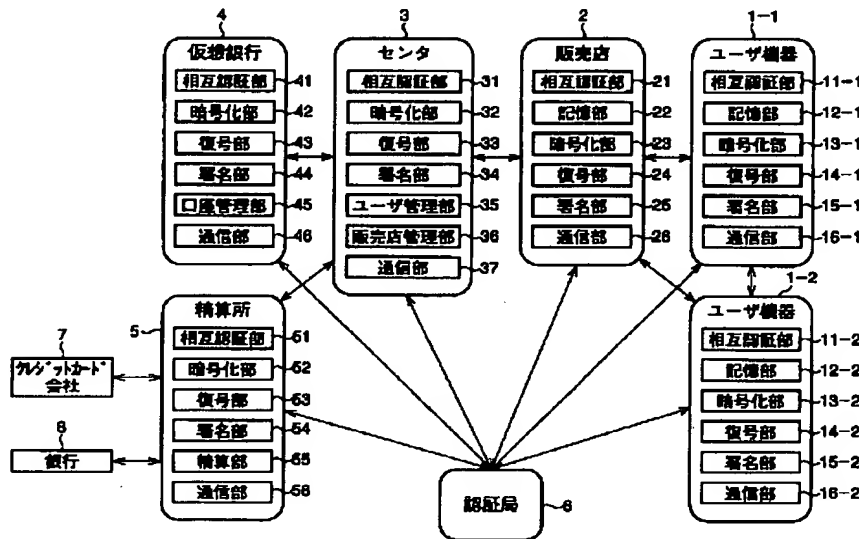
【図8】 ユーザ機器1から販売店2への支払いの処理を説明するフローチャートである。

【図9】 販売店2の口座への売上金の入金の処理を説明するフローチャートである。

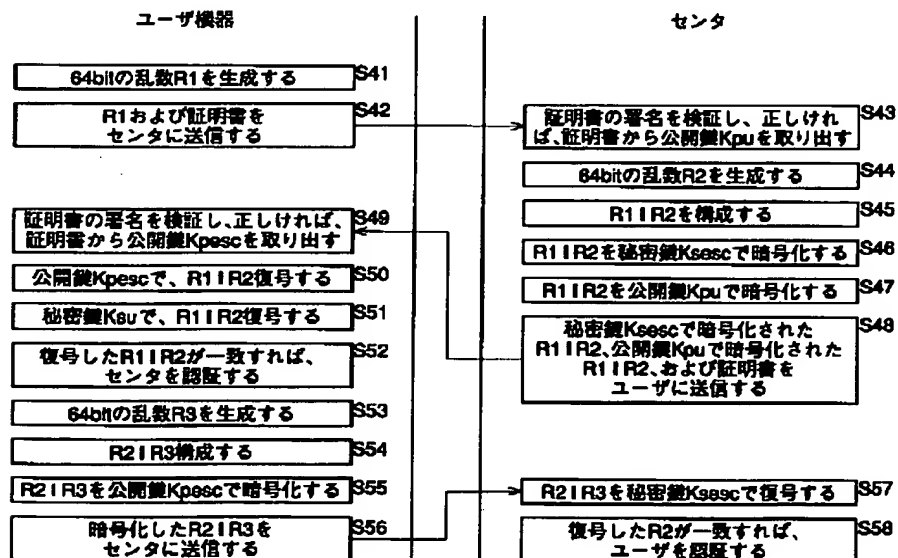
【符号の説明】

1, 1-1, 1-2 ユーザ機器, 2 販売店, 3 センター, 4 仮想銀行, 5 精算所, 35 ユーザ管理部, 37 通信部, 45 口座管理部, 55 精算部

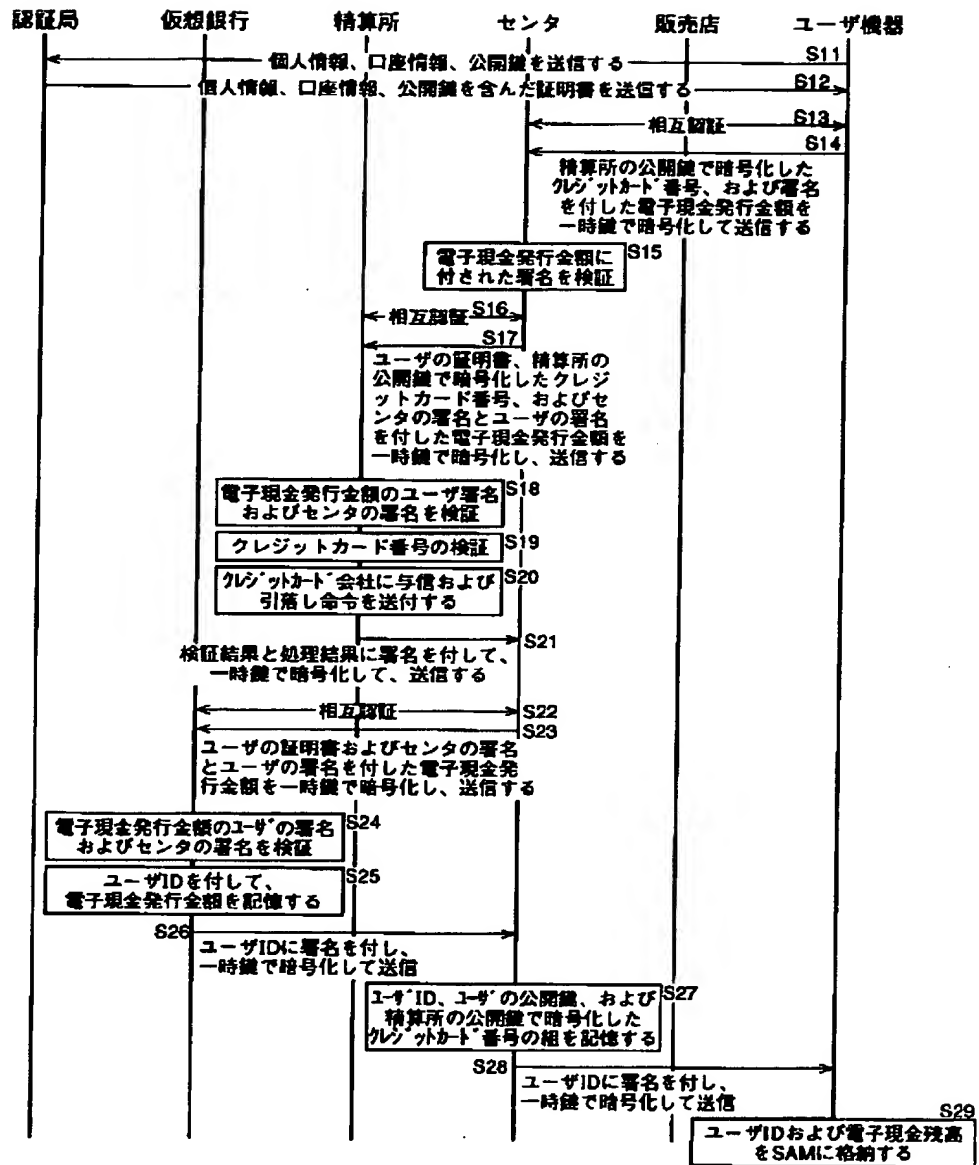
【図1】



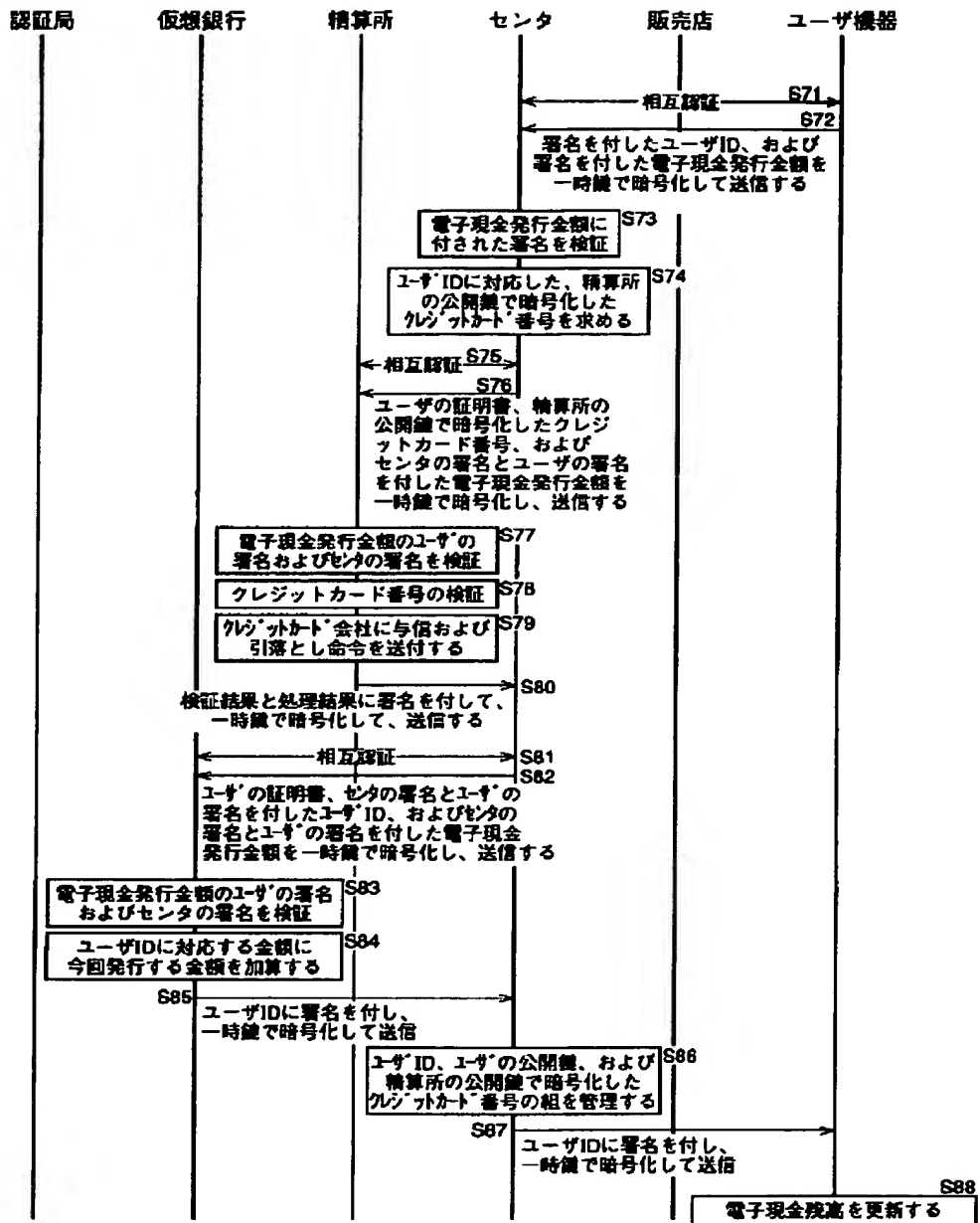
【図3】



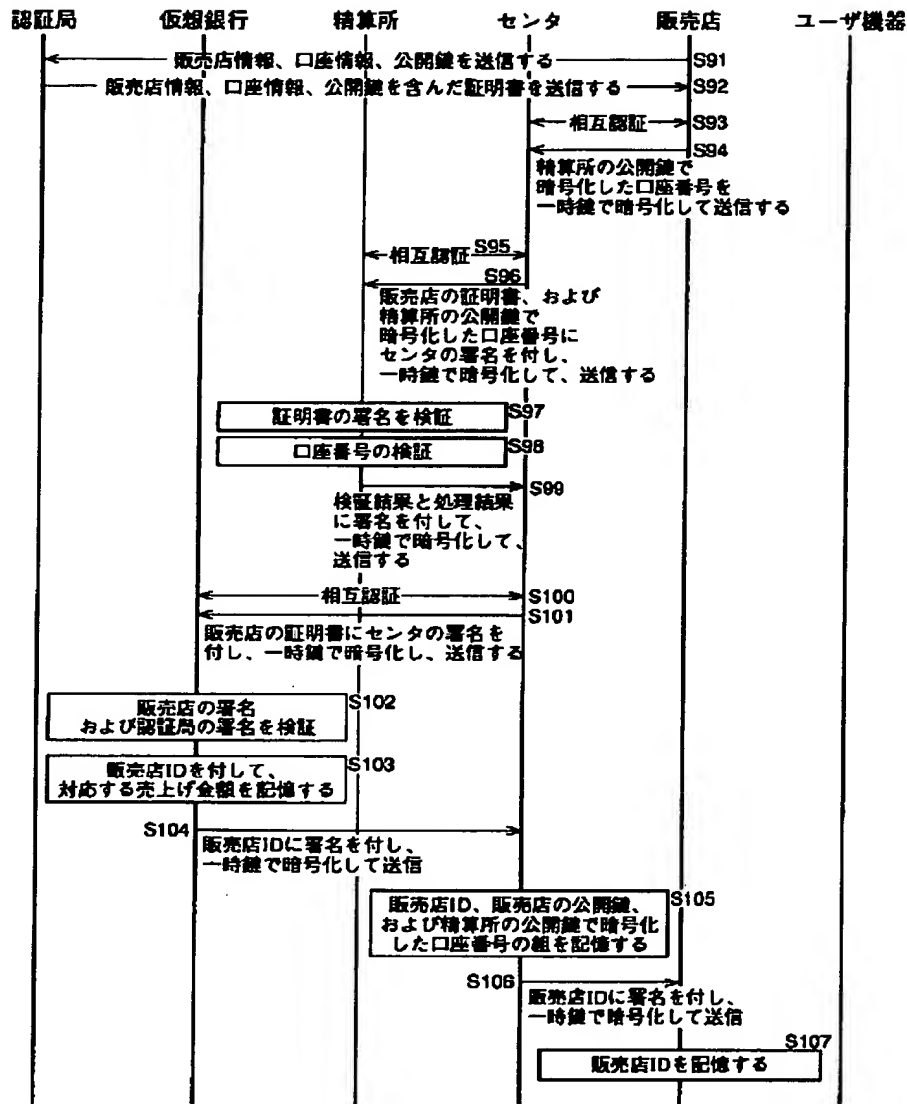
【図2】



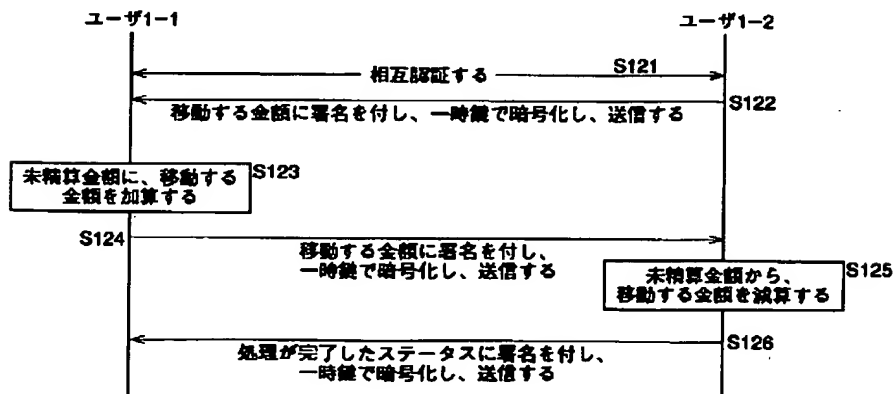
【図4】



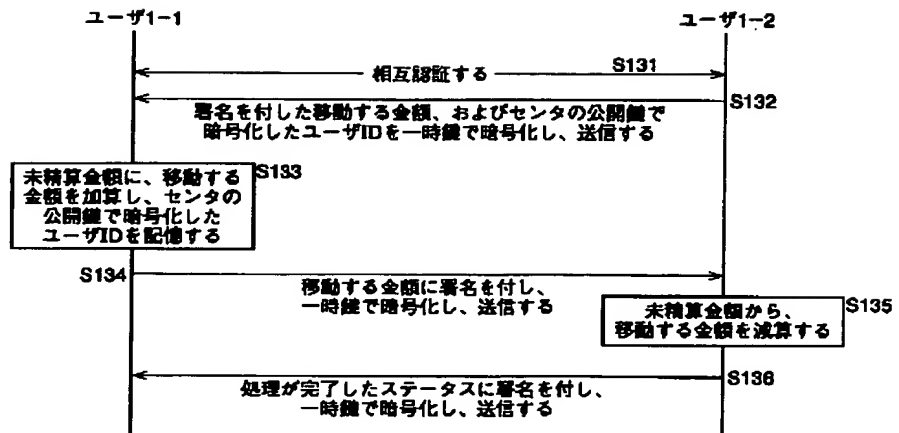
【図5】



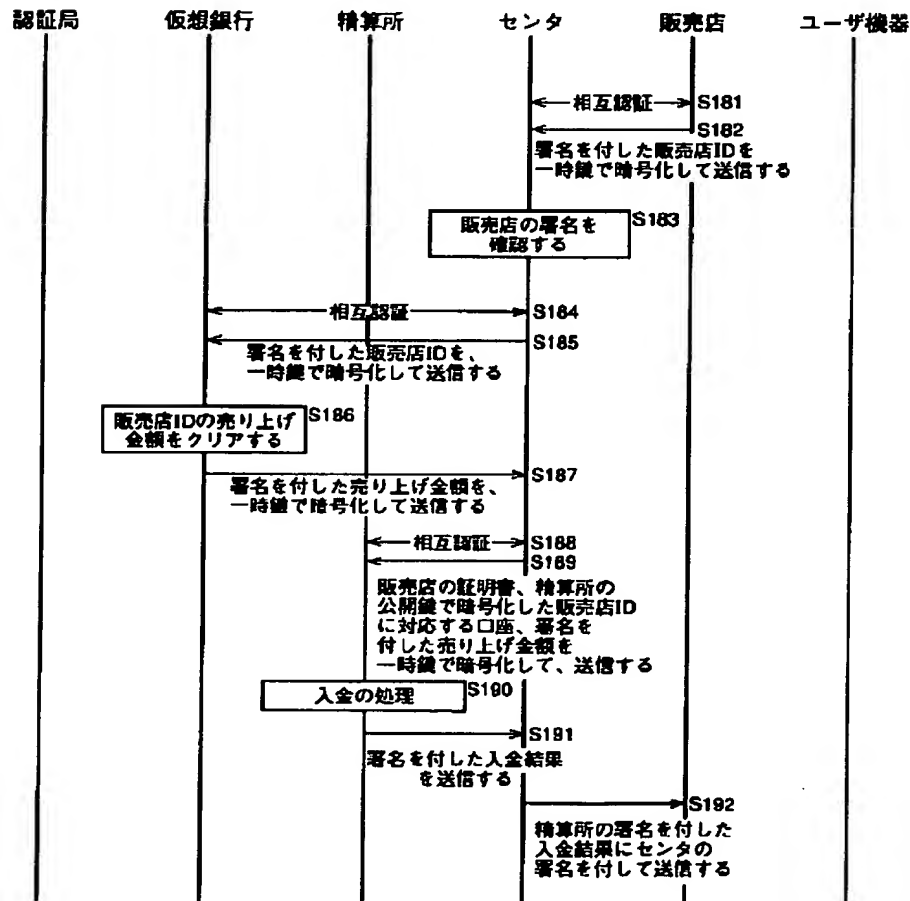
【図6】



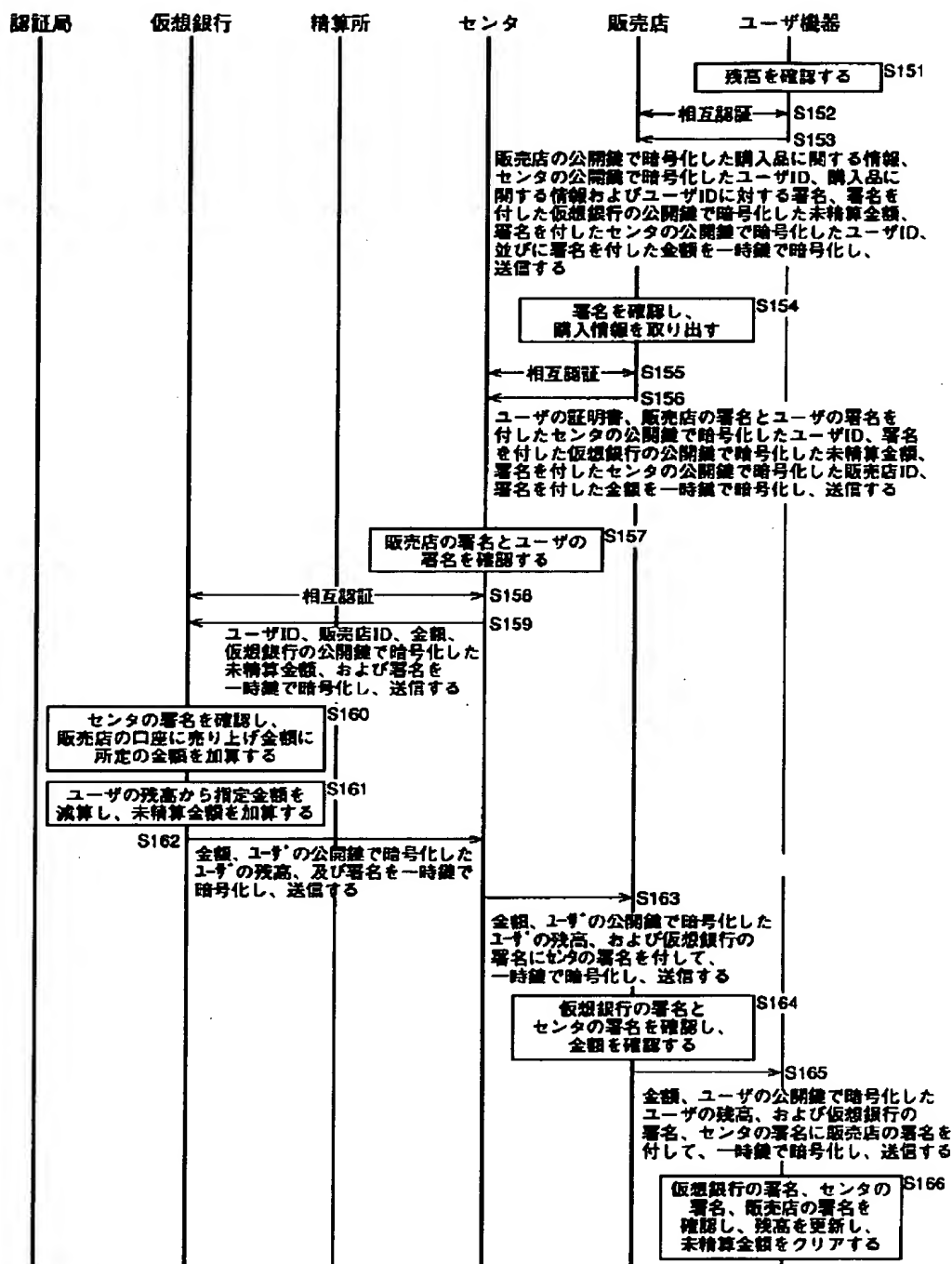
【図7】



【図9】



【図 8】



フロントページの続き

(51)Int.Cl.⁷

G 0 9 C 1/00

識別記号

6 6 0

F I

G 0 6 F 15/30

G 0 7 D 9/00

特マコト*(参考)

L

4 7 6

Fターム(参考) 3E040 BA20 CA14 CA16 DA01
5B049 AA05 BB46 CC36 CC39 EE03
EE09 EE23 EE24 GG04 GG07
GG10
5B055 CB09 EE02 EE03 EE27 FA01
FA05 HA02 HA04 HA12 HB06
HC04 JJ05 KK01 KK09 KK19